REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED

2. Security Classification Authority:

3. Declassification/Downgrading Schedule:

4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.

5. Name of Performing Organization: JOINT MILITARY OPERATIONS DEPARTMENT

6. Office Symbol: C

7. Address: NAVAL WAR COLLEGE
686 CUSHING ROAD
NEWPORT, RI 02841-1207

8. Title:
Critical Vulnerability: Defending the Decisive Point of United States Computer Networked Information Systems (U)

9. Personal Authors: LCDR Roy John Virden, USN

10. Type of Report: FINAL

11. Date of Report: 3 Feb 2003

12. Page Count: 25 **12A Paper Advisor (if any):** Professor David Goodrich

13. Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. Ten key words that relate to your paper: Computer Network Defense, Networked Information Systems, Information Assurance, Defense in Depth, Computer Network Attack, Critical Vulnerability, Information Operations, Information Warfare, Cyber Warfare, Decisive Point

15. Abstract: The reliance on computer networked information systems in every operational function, from operational logistics to intelligence to command and control, has grown in bounds during the last few decades. Electronic transfer of accurate data plays a key role in almost every decision, action and reaction, and is vital for the accomplishment of operational objectives. The military's use of computer networked information systems is thus a critical strength. These systems are then critical vulnerabilities because they may lack adequate protection and are open to enemy attack. Consequently, they could be chosen as a strategic decisive point to a capable opponent.

It can be difficult for a commander to understand the complexity of defending computer networks in a shared risk environment and relatively new state of warfare. The joint force commander's present inexperience with the mechanics and operations of cyber warfare forces too much reliance on the tactical echelon and external organizations to defend and respond to computer network attacks at the operational level.

Examination of Computer Network Defense (CND) doctrine reveals an increased but limited understanding of vulnerability and response issues at the theater-strategic and operational echelons. Operational commanders must be prepared to face the fast paced, quickly advancing, cyber threats of today and tomorrow using yesterday's CND and response doctrine. This thesis presents recommendations at the joint force operational level for improvement in the areas of information systems doctrine, environment, technology, training and organizational structure.

16.Distribution / Availability of Abstract:	**Unclassified**	**Same As Rpt**	**DTIC Users**
	X		

17.Abstract Security Classification: UNCLASSIFIED

18.Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT

19.Telephone: 841-3556	**20.Office Symbol:** **C**

Security Classification of This Page **Unclassified**

NAVAL WAR COLLEGE
Newport, R.I.

CRITICAL VULNERABILITY: DEFENDING THE DECISIVE POINT OF UNITED STATES COMPUTER NETWORKED INFORMATION SYSTEMS

by

Roy John Virden

Lieutenant Commander, U.S. Navy

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: _____

3 February 2003

Signature: _____
Professor David Goodrich
Faculty Advisor

Abstract

The reliance on computer networked information systems in every operational function, from operational logistics to intelligence to command and control, has grown in bounds during the last few decades. Electronic transfer of accurate data plays a key role in almost every decision, action and reaction, and is vital for the accomplishment of operational objectives. The military's use of computer networked information systems is thus a critical strength. These systems are then critical vulnerabilities because they may lack adequate protection and are open to enemy attack. Consequently, they could be chosen as a strategic decisive point to a capable opponent.

It can be difficult for a commander to understand the complexity of defending computer networks in a shared risk environment and relatively new state of warfare. The joint force commander's present inexperience with the mechanics and operations of cyber warfare forces too much reliance on the tactical echelon and external organizations to defend and respond to computer network attacks at the operational level.

Examination of computer network defense (CND) doctrine reveals an increased but limited understanding of vulnerability and response issues at the theater-strategic and operational echelons. Operational commanders must be prepared to face the fast paced, quickly advancing, cyber threats of today and tomorrow using yesterday's CND and response doctrine. This thesis presents recommendations at the joint force operational level for improvement in the areas of information systems doctrine, environment, technology, training and organizational structure.

Introduction

The protection of military information and computer networked information systems is extremely important in achieving strategic and operational objectives. Military networked systems provide the framework or basis of communications allowing person to person and machine to machine transfer of all types of data essential to command and control (C2), intelligence analysis and targeting to name a few. Military networked systems are in place at all levels of warfare: strategic, operational and tactical. The electronic transfer of accurate data plays a key role in almost every decision, action and reaction, and should be considered vital for the accomplishment of a given or assumed military objective. The military's use of computer networked information systems is thus a critical strength. In cases where military objectives can not be achieved without the electronic transfer of information, it can be considered essential in achieving the mission objective. These systems are then critical vulnerabilities because they are open to enemy attack and can represent an operational center of gravity to an opponent. Since this critical vulnerability can be attacked, controlled and used to exercise a marked influence upon a United States military campaign or major operation, it may be considered a strategic decisive point to a capable opponent. It may also be considered a cybernetic decisive point, one an opponent may actively try to penetrate, disrupt, degrade and decapitate within the theater or hundreds of miles away.[1] Therefore, military networked systems must be afforded operational and strategic protection in peacetime, crisis and war to preserve effectiveness and survivability in support of a given theater. Computer network defense (CND) and response is thus a critical foundation in operational protection and maintaining Information Superiority during all modern operational

efforts, while impeding an enemy from destroying, neutralizing or degrading the physical and moral capabilities of one's forces and nonmilitary sources of power.

It can be difficult for a commander to understand the complexity of defending networks in a shared risk environment because of lack of experience and limited staff expertise. Dependence on information systems is a relatively new state of warfare. The joint force commander's present inexperience with the mechanics and operations of cyber warfare results in too much reliance on the tactical echelon and external organizations to respond to computer network attacks at the operational level. Moreover, external organizations assigned to assist with CND are not always familiar with operational information warfare or prepared to respond appropriately.

A more robust philosophy and execution of CND and response at the operational level will provide a marked positive influence on the outcome of campaigns and major operations. Much vulnerability exists therein, and there appears to be insufficient attention given to CND and the protection of military systems. More must be done. In other words, a stronger approach to CND with doctrine, manning, training and organizational structure at the theater-strategic and operational echelons can provide a marked influence on the outcome of campaigns and major operations. The joint force commander needs to know more than it is simply the J-6's responsibility for system restoration once they've been attacked. It is not always the case that systems restoration is the appropriate response. It may be more prudent for the adversary not to degrade the computer networked information systems, but to employ a secrecy attack to collect operational planning or intelligence information. The adversary may also choose an integrity attack, altering logistic, intelligence or targeting data without knowledge of the owner.

The joint force commander needs to take an active approach and be prepared in case his computer networked information systems become a decisive point in the opponent's operational planning. In addition to using Defensive Information Operations (DIO) doctrine as recommended in Joint Publications, the commander needs to also be more aware of the many aspects of CND and response to attacks on his systems. There has been much effort expended and progress made at the tactical level in dealing with appropriate CND and response but little at the operational level. The joint force commander should understand as many options as possible in each facet of CND and response to ensure meeting the strategic and operational objectives are not jeopardized by an adversary's cyber attack.

Military networked information systems and their credibility play an increasingly important role in all facets of planning and executing the commander's estimate. Information systems enhance warfighting capabilities; however, increasing dependence upon rapidly evolving technologies makes joint forces more vulnerable.[2] An ineffectual approach to CND can allow an opponent or intruder to apply offensive computer network attack operations against the integrity of US networked systems. These attacks can result in unauthorized access to privileged information, purposely corrupted critical information or denial of service, preventing or degrading use of our own friendly systems.

Examination of CND doctrine reveals an increased but limited understanding of vulnerability and response issues at the theater-strategic and operational echelons. This paper looks at current operational level protection measures in place, along with vulnerability issues and recommends doctrinal, environment, technology, manning, training and organizational changes at the operational commander level, enhancing CND and response, to better enable the achievement of strategic and operational objectives.

Background

CND, as defined in the Department of Defense Dictionary of Military and Associated Terms, Joint Pub 1-02, includes measures to protect and defend information, computers and networks from disruption, denial, degradation, or destruction.[3] This definition omits an extremely important aspect of CND, protection against unauthorized access to or exploitation of information systems. CND is one form of DIO wherein the theater commander is responsible for combating asymmetric attacks on information systems, infrastructure and other critical areas vulnerable to nontraditional means of attack or disruption within the area of responsibility.[4]

An appropriate and timely response to an attack on computer networked information systems is equally important, if not more important, to an effective effort in CND. With the number of computer network attack vulnerabilities and incidents steadily increasing, it is a given that an organization's computer networked systems will be attacked in some manner. The US Navy experienced more than 16,000 intruders in 2001.[5] The Computer Emergency Response Team (CERT) at Carnegie Mellon, a DoD Defense Advanced Research Projects Agency's computer security organization, reports the number of Internet security incidents increasing on average from 27 per day in 1999 to 268 per day in 2002.[6] Even more serious is the report that new exploitable vulnerabilities, susceptible to attack, increased on average from seven per day in 2001 up to 12 per day in 2002.[7] Now this should not be surprising for at least two major reasons. One reason is that more and more hardware and software is being produced and distributed and as with these many new developments, the removal of all flaws prior to distribution is very difficult, if not impossible. Another reason is that hackers are

becoming more organized and acquiring better technology. Reportedly, al Qaeda and potential adversary nations have sought cyber attack capabilities which likely will surpass those of the average hacker.[8] This demonstrates how being prepared to respond to an information system attack is as important as the initial network defense.

The types of threats to a computer networked information system are as numerous as there are types of systems, and vary from unauthorized access to physical destruction. Most important, perhaps, to the operational level commander are the effects of these attacks on the ability to meet goals and objectives. The effects of any attack can be grouped into one or more of three basic computer security types. These three types are secrecy, integrity and availability. An attack on the secrecy, or confidentiality, of an information system can stem from many common methods of computer network attack, and usually is an unauthorized intrusion by the enemy. Attacks of this type include malicious software[9] locally installed on a computer, access over a network from a remote computer, or even the exploitation of one of today's growing number of wireless networked components such as a laptop computer or handheld personal data assistant (PDA). The obvious danger of a secrecy attack is that the enemy can learn a task force's operational plans and intelligence and then attack appropriately. An integrity, or accuracy, attack of our military sensor, intelligence and targeting systems can lead to maliciously altered data in our databases, which can mislead planning efforts and greatly reduce the effectiveness of operational fires data. An attack on availability, or denial-of-service,[10] can disrupt, degrade or completely stop military systems from functioning, and possibly resulting in a reduced ability to perform C2 functions, delayed logistic transfers or erroneous firing solutions.

All of these effects can be brought on by remote means or even by insider threat.[11] Insiders have legitimate access to military systems, and can attack from within the network of systems, or simply load a malicious program on a connected computer and let it go to work.

Another effect of a computer network attack is the impact on perceptions of vulnerability.[12] Once a single attack has occurred and the trust in the information has been lost, it may be difficult to regain.

Analysis

The reliance on networked information systems in every operational function, from operational logistics to intelligence to C2, has grown during the last few decades. Additionally, advances in technology have been concentrated more in the use of these information systems and with much less concern about protecting them from adversarial attacks. Simply stated, the focus has been in designing and developing new technologies to get the job done rather than taking the time to build in security and protection measures. Thus, resulting vulnerabilities and their potential negative operational impact have led to a demanding need for the joint force commander to be very concerned with the defense of information systems and response to attacks.

Examination of current joint doctrine, directives, DoD instructions and service tactics, techniques and procedures (TTP) at the joint force commander level reveals some reasonable current efforts, but also reveals shortcomings related to computer networked information systems protection measures. Although many aspects in the defense of and response to computer network attacks are addressed, there are many factors which can be

emphasized to help prepare a more informed and capable joint force commander. The areas addressed in this paper are DIO environment and doctrine, technology, proper task force manning, training and education, and organizational structure.

Environment and Doctrine

The Defensive Information Operations chapter of Joint Publication 3-13, Joint Doctrine for Information Operations, is a starting point in the effort to describe the importance of operational protection of the information environment, although it does not go far enough. The publication mentions the importance of DIO integration and coordination of policies, procedures, operations, personnel and technology, but fails to thoroughly explain the many aspects of today's hacker-infested cyber community. The joint force commander must be familiar with these aspects in order to understand the overall operational picture which may include adversarial cyber threats and then be fully prepared with CND and response measures to decisively meet operational objectives. In fact, the term CND is barely mentioned in this doctrinal publication. It is very briefly defined, stating that policies, procedures, hardware and software are necessary when discussing the protection of the information environment.

Joint Publication 3-13 also acknowledges that planners should analyze information systems to determine vulnerabilities to realistic threats, considering both military and nonmilitary systems.[13] This is very important because threats can come from both military and nonmilitary systems, since many of the United States' military networks and nodes are based on a foundation of nonmilitary internets, intranets and major communications

infrastructures. The joint force commander needs to understand this foundation explicitly to effectively respond to cyber information intrusions with the proper level of effort.

Doctrine notes the importance of attack detection and identification, to include monitoring the information systems to watch for attacks as they occur. One of the most important obstacles in computer network intrusion detection and identification is the extremely difficult problem of determining just who the attacker may be. Many attacks against a networked information system are anonymous or are spoofed to appear to be from some unwitting user. A clever adversary could even pose as an allied or coalition member to try to introduce distrust within a combined campaign or operation.

The joint commander is barraged in doctrine with techniques for restoring system capabilities following a destructive attack on joint operations area (JOA) information systems. Many details are provided in the joint publication and include the reliance on backup systems, automated restoration systems and the importance of maintaining a current system resource inventory.[14] All this is extremely important, yet it only addresses one type of attack, the integrity attack. A possibly more devastating attack would be a secrecy attack wherein the enemy does not destroy the operational systems, but steals intelligence, planning or targeting information. And what about an availability or denial of service attack? A denial of service attack could prevent C2 instructions from being promulgated during a time critical phase of an operational maneuver.

When responding to an attack or potential attack, the joint commander is expressly encouraged to identify the attacker in a timely manner, and to recognize that elements of the IO response may include the application of flexible deterrent options. As examples, the commander is advised that other possible response measures include law enforcement,

diplomatic actions, economic sanctions or military force.[15] Yes, these are all very important and valid options, but CND and response planning needs to include the essential requirement of how to continue operations and communications via other mediums which were not affected by the attack. If the primary method of transmitting the next day's air tasking order (ATO) is attacked, by secrecy, integrity or availability, how else can the joint force air component commander (JFACC) inform all the squadrons of their scheduled missions? And what if it was a secrecy attack, and the adversary now knows the scheduled flight plans for the next 72 hours? All these are serious concerns for the joint force commander in accomplishing military objectives. Basically, the virtual world of networked information systems defense and response needs to be incorporated in defense planning, if there is to be any chance of limiting physical damage to in the real world.[16]

The types of attacks or threats to computer networked information systems are alluded to in the joint information operations (IO) publications and practically avoided in DoD CND directives and instructions. The U.S. Navy's TACMEMO, Computer Network Defense for the Navy-Led Joint Task Force, describes, for the Navy joint force commander, four generic categories of attacks as identified by Joint Task Force for Computer Network Operations (JTF-CNO). These four attacks fall into the three basic types of attacks described above, secrecy, integrity and availability. What is omitted, and perhaps even more important to an operational level commander, is not just that threats should be categorized by type of attack, but also categorized by source and destination. This is because the source and destination directly relate to the identification of the attacker and the attacked. The categorization by source and destination are what Shimeall, et al., call the levels of cyber war, three of which are: cyber war as an adjunct to military operations; limited cyber war;

and unrestricted cyber war.[17] The first, cyber war adjunct to military operations, is an attack from an adversary against an opposing military target such as an information processing system or a communications system. The next level, limited cyber war, encompasses an attack on the information infrastructure forcing the military leader to resort to a backup infrastructure with probably even more defense vulnerabilities. The final category, unrestricted cyber warfare, is very widespread. It can include military and civilian targets both on the home front and fighting front with possible physical consequences resulting from attacks on air traffic control or emergency service systems. This type of unlimited cyber war could even result in economic and social impacts.

Technology

There are many aspects of protecting information and information systems, but perhaps none more significant than the technology and equipment on which these systems reside. Current doctrine recognizes this importance, and encourages protection through common policies, procedures and incorporation of technological capabilities, which include physical security measures, vulnerability assessments and other security training.[18] The DoD directive for CND even goes to the point of assigning to the Under Secretary of Defense for Acquisition, Technology and Logistics the responsibility for ensuring that CND requirements are fully integrated into information technology (IT) architectures, plans and programs. There is much more than computer and network material availability that a joint force commander must be aware of to maintain situational awareness when it comes to fighting a cyber war, offensive or defensive. A joint commander should be aware of all the equipment, capabilities and limitations of his armament, whether it be conventional or cyber. Just as

operational commanders do not directly lead an armored brigade into battle, they have an awareness of how many and what kind of opposing tanks can counter or penetrate this line. Similarly, a commander must know the capabilities, limitations and vulnerabilities of his cyber defense and response.

Additionally, the rate of technological advance is extremely fast. Moore's Law says that computer processing power doubles every 18 months.[19] It is important to realize that the vast computer networked information system, which has thousands of pieces, hardware and software, is constantly being upgraded or replaced by newer versions or models. This will challenge any effort to maintain a constant defense. As soon as a system administrator applies all the current vulnerability fixes and patches, a new machine or application will be installed with, of course, new vulnerabilities.

Task Force Manning, Training and Education

Doctrinal direction for the joint force commander emphasizes the need to "develop the skills and abilities required to operate while mitigating joint force vulnerabilities."[20] As an example from one of the Services, the Naval Security Group Command, charged with the initiative to operationalize the Navy's CND, understands that effective CND requires skilled planners and operators integrated throughout the fleet and shore infrastructure. Yet there is a "lack of sufficient numbers of trained, skilled personnel… to ensure Navy CND professionals remain technically competent in the constantly changing continuum of Information Security."[21] This is a very difficult problem and can greatly affect a joint commander leading a force comprised of all the Services. It takes much time and money to

educate and train with experience a continuously flowing workforce on a technology that flows at even a much quicker pace.

Also inherent, and with possible negative impact to a joint force as a whole, are the military personnel deployment schedules, wherein force expertise and experience will roll-in and roll-out of a JOA. It can take months or years to get a person trained and ready to handle the high technology knowledge requirements needed to actively defend such a large computer network infrastructure. Once the resources are spent to get them trained, they do their six month deployment aboard ship, or in the field, and then return to their home port and the temptation to finish out their term and shift to the highest bidder in the commercial IT market.

Organizational Structure

Just who is responsible for a joint force commander's CND? The Joint Task Force for Computer Network Operations (JTF-CNO) originated, in 1998, after a series of exercises and real-world cyber events that targeted critical DoD networks and demonstrated that mission essential networks were at risk. After a number of name changes and mission expansions, JTF-CNO was assigned as the United States Space Command (SPACECOM) (now within United States Strategic Command (STRATCOM)) operational entity for both network defense and network attack in April, 2001. JTF-CNO is responsible for coordinating and directing the defense of DoD computer systems and networks, and directing appropriate actions through its four military service components and the DoD CERT over each service's computer emergency response team.[22] However, each combatant commander, Service and Agency still holds the responsibility to develop their own internal processes and to ensure

their own information systems and networks are defended. So, where does the joint force commander turn for operational CND and response guidance? STRATCOM and the JTF-CNO maintain a liaison officer (LNO) at each geographic combatant commander Headquarters (normally within the J3 operations directorate) to coordinate computer network operations support. During crisis operations, the LNO can be augmented with computer network experts to form a SPACECOM Information Operations Element (SIOE) within the combatant commander headquarters. As a result, because of disjointed CND Service components and separation from the LNO, the joint force commander is perhaps not best suited to maintain positive operational control regarding CND and response. First, the commander has separate service components manning computer network defensive positions within the JOA. Since each of the services maintain their own defensive standards they are unlikely at equal levels of proficiency and protection. Second, the joint force commander may only have remote access to the combatant commander's CND LNO and possibly a team of visiting experts who may or may not be familiar with the area of responsibility. And finally, the combatant commander's CND LNO, who has a connection to another unified commander, STRATCOM, may have overriding national objectives which could conflict with local operational objectives.

How do we solve these problems?

Improvements in CND and response are progressing, most notably on the tactical level, where information system users and administrators handle the day-to-day application of the latest vulnerability fixes. Yet, as these front line cyber warriors are improving security techniques, the threats and vulnerabilities continue to escalate daily. However, the

operational level commander is not progressing as adequately. While the joint commander uses operational functions, such as operational C2 and operational maneuver, to achieve objectives through networked communications or the transfer of critical data, those operational functions rely heavily on computer networked information systems. These systems can be operational decisive points to the technically adept enemy. Therefore, operational commanders must demand a better introduction to information systems defense and response through doctrine, environment, training and organizational structure.

Environment and Doctrine

The IO environment is expansive and ever growing. As more and more people from all countries throughout the world gain access to the Global Information Infrastructure (GII),[23] the numbers of possible attackers also increases. The joint force commander may not fight battles totally in cyberspace, but will certainly make use of it everyday and in every operational function. The commander who facilitates successful military operations and campaigns must know all aspects of the environment. Therefore, doctrine must be thorough and complete to provide operational leaders the knowledge they need especially in today's virtual environment which is extremely new and still full of many unknowns.

Doctrine must address the full spectrum of the environment. It needs to cover the who, what, when, where, why and how of modern cyber warfare. Now, as stated, this is not easy, because it is a new component of warfare. The joint commander must demand a staff adept not just at conventional operational planning, but also knowledgeable and experienced with the cyber environment, capabilities and, most importantly at this stage, appropriate defensive responses. Currently, a complete, impenetrable CND is impossible to attain. And

once the network is attacked and unusable, are the users prepared to continue fighting without that functioning network and connectivity? Doctrine must reflect the defense of the new and complex environment, as well as, the myriad of responses required to successfully counter enemy cyber attacks. Once a commander is comfortable with appropriate responses, they must be conveyed in planning orders to allow subordinate commands to also be prepared.

Doctrine must be documented quickly, as more is learned in this fast paced environment. It must document not simply who the enemy is, but how they might appear in a virtual world. Are they sophisticated? Normally they are anonymous and difficult to identify. Will the attacks favor the aggressor? Presently most attacks favor the aggressor, because they are difficult to detect and we are not prepared. It is currently impossible to shield off every attack because the speed at which vulnerabilities and exploits appear is quicker than our ability to put defensive measures and fixes in place. Therefore, the commander needs to insist that doctrine is complete and up to date, and then test it. Information systems vulnerability assessments[24] can be conducted using capable, existing red teams[25] that pose as the adversary during joint force exercises or in independent testing. It is current practice to employ cyber red teams, but normally their actions are very limited to allow blue team mission accomplishment during the exercise.

Where do the threats originate and what types of attacks can be conducted? This is partially addressed in doctrine, as previously discussed, but is incomplete. The source of an attack is very important for the commander who must ensure the entire Joint Planning Group has a full understanding of all aspects of the cyber environment. The source of the attack is important because, aside from determining the appropriate action based on attacker's origin,

diplomatic rules of engagement may override the military response. Doctrine must be complete.

Technology

Although most software and hardware acquisition or budgetary issues are out of the joint task force's control, the commander does need to understand that many hardware and software components do exist and are under separate control of each military service. The commander does not need to know how many network servers or operating systems have been installed in the theater, but does need to know that defensive capabilities vary and that vulnerabilities exist which, if successfully attacked, can seriously hinder the accomplishment of operational objectives. In order to be considered during planning, all of the capabilities, their limitations, and susceptibility to computer network attack must be known to the Joint Planning Group.

Task Force Manning, Training and Education

As with any skill, but especially skills involved with the new frontier of the cyber world, training is paramount. Training in all forms needs to be addressed and practiced, and not just at the tactical level. Operational planners and leaders need to practice and experience, at the operational level, the relationships between the processes of operational functions, such as C2, intelligence, fires and protection, and their reliance on the interconnectivity of computer networked information systems.

Organizational Structure

Fitting a joint task force staff with CND and response representatives is difficult right now and not just because of the lack of training. As discussed, the current entity responsible for CND may be thousands of miles away at the JTF-CNO headquarters or may be hundreds of miles away working on the combatant commander's staff. Moreover, the service components information warfare centers are located in the continental United States. The joint force commander should insist on additional permanent staff personnel with some form of cyber attack, defense and response expertise within the joint task force planning and operation centers. This expertise would certainly be a part of the designated IO cell. As stated in the joint pubs, "the JFC normally will assign responsibility for IO to a member of the joint staff, usually the J-3, who is responsible for planning, coordinating and integrating joint force IO."[26] Additionally, an IO Officer is designated to support the J-3. There is no recommendation in doctrine that the J-3 representative or IO Officer be trained in any IO facet, let alone CND and response. IO cell doctrine also recommends representation from the J-2 through J-7, a psychological operations group (PSYOP), electronic warfare (EW), operational security (OPSEC), Deception, etc., yet there is no mention of needing a representative in the area of CND and response. The joint force commander, through combatant commander support, must include this representation to be best prepared for the total cyber threat.

Conclusion

The joint force commander is in a position to continuously experience the execution and results of vulnerabilities and attacks. Within the past few days, a presently unknown

attacker released a virus-like worm which shut down 13,000 major US bank automated teller machines , caused airline delays and cancellations, and invaded government and military servers. Additionally, as a result of this attack, millions of Internet users were affected around the world in places like South Korea, Japan and Finland.[27] Operational commanders must be prepared to face the fast paced, quickly advancing, cyber threats of today and tomorrow using yesterday's CND and response doctrine. The shortcomings in the current operational level doctrine can be overcome with a reasonable amount of attention in the areas of information systems environment, technology, training and organizational structure.

Notes

[1] Milan N. Vego, Operational Warfare (Newport RI: Naval War College, 2000), 167.

[2] Joint Chiefs of Staff, Joint Doctrine for Information Operations, Joint Pub 3-13 (Washington, DC: 9 October 1998), III-1.

[3] Joint Chiefs of Staff, Department of Defense Dictionary of Military and Associated Terms, Joint Pub 1-02 (Washington, DC: 14 August 2002), 93.

[4] Milan N. Vego, Operational Warfare (Newport RI: Naval War College, 2000), 280.

[5] RADM Charles L. Munns, US Navy, "A Global Navy Needs a Global Network," U.S. Naval Institute Proceedings (January, 2003): 60.

[6] "CERT/CC Statistics 1988-2002," 4 October 2002, <www.cert.org/stats/> [1 December 2003].

[7] ibid.

[8] RADM Charles L. Munns, US Navy, "A Global Navy Needs a Global Network," U.S. Naval Institute Proceedings (January, 2003): 60.

[9] Malicious software: Computer security software programs or code, such as viruses, worms, Trojan horses, trap doors, etc., designed to cause an undesired or unintended effect on a computer or network system. Deborah Russell and G.T. Gangemi Sr., Computer Security Basics (Sebastopol, CA: O'Reilly & Associates, Inc., 1992), 79.

[10] Availability attack, denial of service: An attack on availability or a denial of service attack is intended to affect a computer or network's system resources greatly reducing throughput and efficiency, perhaps even resulting in a complete system halt. These can prevent the functional use of the attacked system until capabilities are restored. Deborah Russell and G.T. Gangemi Sr., Computer Security Basics (Sebastopol, CA: O'Reilly & Associates, Inc., 1992), 10.

[11] Insider threat: The primary threat to computer systems has traditionally been the insider attack. Insiders are likely to have specific goals and objectives, and have legitimate access to the systems. Insiders can plant malicious code or browse through the files systems. This type of threat can be extremely difficult to detect or protect against. Arthur E. Hutt and others, Computer Security Handbook, (New York: John Wiley & Sons, Inc., 1995), A23.8.

[12] Milan N. Vego, Operational Warfare (Newport RI: Naval War College, 2000), 280.

[13] Joint Chiefs of Staff, Joint Doctrine for Information Operations, Joint Pub 3-13 (Washington, DC: 9 October 1998), III-7.

[14] Current system resource inventory: A current system resource inventory includes all software applications, file systems and database entries which can be used to rebuild an organization's computer information system following the destruction of partial or full capability.

[15] Joint Chiefs of Staff, Joint Doctrine for Information Operations, Joint Pub 3-13 (Washington, DC: 9 October 1998), III-14.

[16] Timothy Shimeall, Phil Williams and Casey Dunleavy, "Countering cyber war," NATO Review (Winter 2001/2002), 18.

[17] ibid, 17.

[18] Joint Chiefs of Staff, Joint Doctrine for Information Operations, Joint Pub 3-13 (Washington, DC: 9 October 1998), III-8.

[19] T.G. Lewis, The Friction-Free Economy (New York: Harper Business, 1997), 6.

[20] Joint Chiefs of Staff, Joint Doctrine for Information Operations, Joint Pub 3-13 (Washington, DC: 9 October 1998), III-5.

[21] Naval Security Group Command, PR-05 Claimant Issue Paper on Operationalizing Navy Computer Network Defense (Washington, DC: 2002), Enclosure 3, p 4.

[22] Strategic Command, Fact File, 30 September 2002, <http://www.stratcom.af.mil/factsheetshtml/jtf-cno.htm> [25 January 2003].

[23] Global Information Infrastructure: The worldwide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. The global information infrastructure encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, fiber-optic transmission lines, networks of all types, televisions, monitors, printers, and much more. The friendly and adversary personnel who make decisions and handle the transmitted information constitute a critical component of the global information infrastructure. Joint Chiefs of Staff, Joint Doctrine for Information Operations, Joint Pub 3-13 (Washington, DC: 9 October 1998), GL-6.

[24] Vulnerability assessments: In information operations, a systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. Department of Defense, Support to Computer Network Defense, DoD Instruction O-8530.2 (Washington, DC: 8 January 2001), 13.

[25] Red Team: An independent threat based activity aimed at readiness improvements through simulation of an opposing force. Red teaming activity includes becoming knowledgeable of a target system, matching an adversary's approach, gathering appropriate tools to an attack the system, training, launching an attack, then working with system owners to demonstrate vulnerabilities and suggest countermeasures. Department of Defense, Support to Computer Network Defense, DoD Instruction O-8530.2 (Washington, DC: 8 January 2001), 13.

[26] Joint Chiefs of Staff, Joint Doctrine for Information Operations, Joint Pub 3-13 (Washington, DC: 9 October 1998), IV-2.

[27] CNN Web Site, Computer worm grounds flights, blocks ATMs, 25 January 2003, <http://www.cnn.com/2003/TECH/internet/01/25/internet.attack/index.html> [26 January 2003].

BIBLIOGRAPHY

"CERT/CC Statistics 1988-2002." 4 October 2002. <http://www.cert.org/stats/> [12 January 2003].

"CERT Coordination Center 2001 Annual Report." 19 February 2002. <http://www.cert.org/annual_rpts/cert_rpt_01.html> [12 January 2003].

Clausewitz, Carl von. On War. Michael Howard and Peter Paret eds. and trans. Princeton: Princeton University Press, 1984.

CNN Web Site. "Computer worm grounds flights, blocks ATMs." 25 January 2003. <http://www.cnn.com/2003/TECH/internet/01/25/internet.attack/index.html> [26 January 2003].

Dahl, Eric J. "Network Centric Warfare and the Death of Operational Art." Unpublished JMO Faculty Paper, U.S. Naval War College, Newport, RI: September 2001.

Dean, Joshua. "Feds get 'F' in computer security." 09 November 2001. <http://www.govexec.com/dailyfed/1101/110901j1.htm> [08 May 2002].

Denning, Dorothy E. Information Warfare and Security. Reading, MA: Addison-Wesley, 1999.

Helms, Chet, Captain. Operational Functions. Unpublished JMO Paper, U.S. Naval War College, Newport, RI: n.d.

Hutt, Arthur E., Seymour Bosworth and Douglas B. Hoyt. Computer Security Handbook. New York: John Wiley & Sons, Inc., 1995.

Lewis, T.G. The Friction-Free Economy. New York: Harper Business, 1997.

Metz, Stephen. Armed Conflict in the 21st Century: The Information Revolution and Post Modern Warfare. US Army War College Strategic Studies Institute. Carlisle, PA, U.S. Army War College: April 2000.

Munns, Charles L., RADM, US Navy. "A Global Navy Needs a Global Network." U.S. Naval Institute Proceedings (January, 2003): 60.

Russell, Deborah and G.T. Gangemi, Sr. Computer Security Basics. Sebastopol, CA: O'Reilly & Associates, Inc., 1992.

"SANS Institute." 14 May 1999. <http://www.sans.org/resources/errors.php> [20 January 2003].

Shimeall, Timothy, Phil Williams and Casey Dunleavy. "Countering cyber war." NATO Review, Winter 2001/2002.

Smith, Edward A., Jr. "Network-Centric Warfare: What's the Point?" Naval War College Review, Winter 2001.

U.S. Commission on National Security/21st Century. New World Coming: American Security in the 21st Century, Major Themes and Implications (Phase I Report). 15 September 1999.

U.S. Department of Defense. Computer Network Defense. DoD Directive O-8530.1. Washington, DC: 8 January 2001.

U.S. Department of Defense. Support to Computer Network Defense. DoD Instruction O-8530.2. Washington, DC: 8 January 2001.

U.S. Joint Chiefs of Staff. Department of Defense Dictionary of Military and Associated Terms, Joint Pub 1-02. Washington, DC: 14 August 2002.

U.S. Joint Chiefs of Staff. Doctrine for Intelligence Support to Joint Operations, Joint Pub 2-0. Washington, DC: 9 March 2000.

U.S. Joint Chiefs of Staff. Doctrine for Joint Operations, Joint Pub 3-0. Washington, DC: 10 September 2001.

U.S. Joint Chiefs of Staff. Joint Doctrine for Command and Control Warfare (C2W), Joint Pub 3-13.1. Washington, DC: 7 February 1996.

U.S. Joint Chiefs of Staff. Joint Doctrine for Information Operations, Joint Pub 3-13. Washington, DC: 9 October 1998.

U.S. Joint Chiefs of Staff. Joint Vision 2020, America's Military: Preparing for Tomorrow. n.d.

U.S. Joint Chiefs of Staff. National Military Strategy of the United States of America. Washington, DC: September 1997.

U.S. Naval Security Group Command. PR-05 Claimant Issue Paper on Operationalizing Navy Computer Network Defense. Washington, DC: 2002.

U.S. Navy, Fleet Information Warfare Center. Computer Network Defense (CND) for the Navy-Led Joint Task Force. TACMEMO 3-13.01-02. n.d.

U.S. President. The National Security Strategy of the United States of America. Washington, DC: September 2002.

U.S. Representatives. House. Committee on Armed Services. Examining Vulnerabilities Of Department Of Defense Networks: Hearings before the Committee on Armed Services. 107th Congress, 1st Session, 17 May 2001.

U.S. Strategic Command, Fact File. 30 September 2002. <http://www.stratcom.af.mil/factsheetshtml/jtf-cno.htm> [25 January 2003].

Vego, Milan N. Operational Warfare. U.S. Naval War College, Newport, RI: 2000.